Supplementary materials for the paper
Efficient Quantum Pseudorandomness

Fernando G.S.L. Brandão,[1] Aram W. Harrow,[2] and Michał Horodecki[3]

[1]Microsoft Research Redmond & Computer Science Department, University College London
[2]Center for Theoretical Physics, Massachusetts Institute of Technology
[3]National Quantum Information Center of Gdansk

In the main paper, we referred to a result due to Nachtergaele [1] that permits the spectral gap of an n-body Hamiltonian to be bounded in terms of the gap of an m-body Hamiltonian for m potentially much smaller than n. Here we define precisely this result and show how it can be applied to the $H_{n,k}$ appearing in our model.

We consider a chain of systems with local finite-dimensional Hilbert space $\mathcal{H}$ labeled by positive integers. We consider a family of Hamiltonians

$$H_{[m,n]} := \sum_{i=m}^{n-1} h_{i,i+1} \tag{1}$$

acting on $\mathcal{H}^{\otimes(n-m)}$, where $h_{i,i+1}$ are the nearest neighbor interaction terms, which are assumed to be projectors. In words, $H_{[m,n]}$ includes all the interactions terms for which both systems belong to the interval $[m,n]$. We also let the chain be translationally invariant, i.e. $h_{i,i+1}$ are the same for all i. We assume further that the minimum eigenvalue of $H_{[m,n]}$ is zero for all m,n and denote by $\mathcal{G}_{[m,n]}$ the ground space of $H_{[m,n]}$, namely

$$\mathcal{G}_{[m,n]} = \{|\psi\rangle \in \mathcal{H}^{\otimes(n-m+1)} \ \ : \ \ H_{[m,n]}|\psi\rangle = 0\}. \tag{2}$$

Finally let $P_{[m,n]}$ be the projector onto $\mathcal{G}_{[m,n]}$.

Lemma 1 (Nachtergaele, Theorem 3 of [1]). *Suppose there exist positive integers l and n_l, and a real number $\epsilon_l \leq 1/\sqrt{l}$ such that for all $n_l \leq m \leq N-1$,*

$$\|I_{A_1} \otimes P_{A_2B}\left(P_{A_1A_2} \otimes I_B - P_{A_1A_2B}\right)\|_\infty \leq \epsilon_l \tag{3}$$

with $A_1 := [1, m-l-1]$, $A_2 := [m-l, m-1]$, $B := m$. Then

$$\Delta(H_{[1,n]}) \geq \Delta(H_{[1,l]})\left(\frac{(1-\epsilon_l\sqrt{l})^2}{l-1}\right). \tag{4}$$

It remains to prove that (3) holds for P_X of the form $\mathbb{E}_{\text{Haar}} U^{\otimes k,k}$.

The Structure of $H_{n,k}$: It turns out that $H_{n,k}$ has a few special properties which make the estimation of its spectral gap feasible. Here we use basic facts about representation theory of the symmetric group to show:

Lemma 2. *For every $n,k > 0$ the following properties of $H_{n,k} = \sum_i (I - P_{i,i+1})$ hold:*

1. *the minimum eigenvalue of $H_{n,k}$ is zero and the zero eigenspace is given by*

$$\mathcal{G}_{n,k} := span\left\{|\psi_\pi\rangle^{\otimes n} : \ \pi \in S_k\right\}, \tag{5}$$

$$|\psi_\pi\rangle := (I \otimes V(\pi))|\Phi_{2^k}\rangle \tag{6}$$

with $|\Phi_{2^k}\rangle := 2^{-k/2}\sum_{i=1}^{2^k}|i,i\rangle$ the maximally entangled state on $(\mathbb{C}^2)^{\otimes k} \otimes (\mathbb{C}^2)^{\otimes k}$, S_k the symmetric group of order k, and $V(\pi)$ the representation of the permutation $\pi \in \mathcal{S}_k$ which acts on $(\mathbb{C}^2)^{\otimes k}$ as

$$V(\pi)|l_1\rangle \otimes ... \otimes |l_k\rangle = |l_{\pi^{-1}(1)}\rangle \otimes ... \otimes |l_{\pi^{-1}(k)}\rangle; \tag{7}$$

2. *Let $P_{n,k}$ be the projector onto $\mathcal{G}_{n,k}$. If $k^2 \leq 2^n$, then*

$$\sum_{\pi \in \mathcal{S}_k} |\langle\psi_\sigma|\psi_\pi\rangle|^n \leq 1 + \frac{k^2}{2^n}, \qquad \forall \sigma \in \mathcal{S}_k \tag{8}$$

and

$$\left\| \sum_{\pi\in\mathcal{S}_k} |\psi_\pi\rangle\langle\psi_\pi|^{\otimes n} - P_{n,k}\right\|_\infty \leq \frac{k^2}{2^n}. \tag{9}$$

The key non-trivial fact here is the quasi-orthogonality property of the states $|\psi_\pi\rangle$ given by Eqs. (8) and (9), which will be used to derive a good lower bound on the spectral gap of $H_{n,k}$. Intuitively, (8) states that the set $\{|\psi_\pi\rangle : \pi \in \mathcal{S}_k\}$ is approximately orthogonal. Thus we have (9), which states that $\sum_\pi |\psi_\pi\rangle\langle\psi_\pi|$ is approximately equal to the projector onto its support, i.e. $P_{n,k}$. Suppose these states were *exactly* orthogonal and the sum $\sum_\pi |\psi_\pi\rangle\langle\psi_\pi|$ was exactly equal to $P_{n,k}$. Then a straightforward calculation would yield that (3) holds with $\epsilon_l = 0$. Since we only have approximate equality, we instead obtain (3) with $\epsilon_l = O(k^2/2^n)$. This means that taking $l \gg 2\log(k)$ allows us to bound $\Delta(H_{n,k})$ in terms of $\Delta(H_{l,k})$.

The proof of Lemma 2 and additional details about the proof of the main theorem can be found in [2].

[1] B. Nachtergaele, Communications in Mathematical Physics **175**, 565 (1996), arXiv:cond-mat/9410110.

[2] F. G. S. L. Brandão, A. W. Harrow, and M. Horodecki, *Local random quantum circuits are approximate polynomial-designs* (2012), arXiv:1208.0692.